UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,850	09/30/2003	Nicholas M. Ryan	2222.5440000	3054

26111 7590 04/03/2012

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
04/03/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/676,850	RYAN, NICHOLAS M.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-22 and 26-34* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-22 and 26-34* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/23/2012*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's submission for RCE filed on 2/23/2012 has been entered. Currently claims 1-22 and 26-34 are pending in this application.

Response to Arguments

Applicant's arguments filed 02/23/2012 have been fully considered but they are not persuasive.

Claims 1 and 3:

Applicant argues that, "According to the claim features recited in claim 1, "the access manager is configured to require that the requestor use the private key pertaining to the predetermined time to access a document key in *an encrypted header* of a secured electronic file, a data portion of the secured electronic file which was previously secured using the document key, and wherein the header includes the document key and access rules for the secured electronic file, *the access rules configured to further protect the document key."* However, according to Narasimhalu, *a decrypted header* includes AW 37, TAL 38 and LAL 39, and they are not taught to further protect K1 to KTAL 41. AW, TAL and LAL are taught to merely protect the body."

In response, examiner would like to point out that applicant appears to argue that the decrypted header includes AW 37, TAL 38 and LAL 39 and not the encrypted header which is not persuasive. Because from fig. 2 it is clear that encrypted header include AW 37, TAL 38 and LAL 39 which becomes accessible to visible upon decryption. Furthermore, Narasimhalu clearly discloses encrypting AW 37, TAL 38 and

LAL 39 in an encrypted header (see, Column 2, lines 59-62 and also Column 6, lines 22-45, "Initially the value LAL 39 is set to be identical with that of TAL 38. By concatenating AW 37, TAL 38, LAL 39, K.sub.1 to K.sub.TAL 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device".). Therefore, applicant's argument that only the decrypted header contains AW 37, TAL 38 and LAL 39 is not found persuasive. In response to applicant's arguments that AW 37, TAL 38 and LAL are not taught to further protect K1 to KTAL 41. AW, TAL and LAL are taught to merely protect the body, examiner would like to point out that Fig. 5A and Column 7, lines 29-65 discloses that keys are only extracted when the LAL (legal access left) is not zero, access window AW is within the time boundary and further check if the signature is correct. IF all these conditions (access rules) are satisfied only then keys are extracted. Therefore, Narasimhalu clearly discloses "the access rules configured to further protect document key".

Applicant further argues that, "In the previous response, Applicant noted that AW, TAL and LAL do not protect K1 to KTAL before the header of Narasimhalu is unencrypted. In addition, they also do not protect K1 to KTAL after the header is unencrypted, because they merely protect the body. Applicant was merely pointing out that Narasimhalu's AW, TAL and LAL fail to protect K1 to KTAL, rather they work in conjunction with AW, TAL and LAL to protect the body. Figure 2 of Narasimhalu shows how the header is decrypted and the keys are in the clear. (Narasimhalu, 7:25-48, 7:61-65, FIG. 2 and FIG. 5A: "After the Controller 45 determines that the Information

Consumer 30 has a right to access the sealed COIN on the distribution medium in FIG. 5A, the controller extracts in step 95 the encryption decryption key KTAL-LAL+I from the header 35.") Thus, Narasimhalu fails to teach *"an encrypted header* of a secured electronic file, a data portion of the secured electronic file which was previously secured using the document key, and wherein the header includes the document key and access rules for the secured electronic file, *the access rules configured to further protect the document key."*

Applicant's argument that since keys are in clear the access rule cannot protect the keys is not persuasive because as pointed out above, Narasimhalu in Fig. 5A and Column 7, lines 29-65 discloses that keys are only extracted when the LAL (legal access left) is not zero, access window AW is within the time boundary and further check if the signature is correct. If all these conditions (access rules) are satisfied only then keys are extracted. It appears that applicant is arguing that access rules protect the key from being decrypted but current claim language only require access rule to protect the document key which so broad that a controlled extraction of the keys can be interpreted as "protecting" the key. Furthermore, to facilitate comparing the claim language with the prior art, examiner would like to advise applicant to point out exactly how access rules protect the document keys in the current inventions.

Applicant's other argument regarding at least one of the cryptographic key pairs pertaining to a predetermined time, being uniquely generated each day have been fully considered and persuasive. Therefore, the rejection has been withdrawn. However,

upon further consideration, a new ground(s) of rejection is made in view of Friedman (see rejection below).

Claims 2, 4 and 5:

Applicant does not submit separate arguments for claims 2, 4, and 5 but relies on the arguments made with respect to claim 1.

Claims 6-13, 15-17, 20-22, and 26-31:

Applicant does not submit separate arguments for claims 6-13, 15-17, 20-22 and 26-31 but relies on the arguments made with respect to claim 1.

Claims 14, 18 and 19:

Applicant does not submit separate arguments for claims 14, 18 and 19 but relies on the arguments made with respect to claim 1.

Claims 32-34:

Applicant's arguments regarding claims 32 have been fully considered and persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Bryan (see rejection below).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley (US 6,292,895 B1), hereinafter "Baltzley" in view of Angelo et al. (US 5,923,754), hereinafter, "Angelo", and Friedman et al. (US 2002/0019933 A1), "Friedman", and further in view of Narasimhalu et al. (US 5,499,298), hereinafter, "Narasimhalu".

Regarding **Claim 1**, Baltzley discloses a file security system for restricting access to electronic files, said file security system comprising:

a key store configured to store a plurality of cryptographic key pairs, wherein the cryptographic key pairs include a respective public key and a respective private key (see, Fig. 2, Numerals 320, and 325).

an access manager (see Fig. 3, Numeral 220), configured to operatively connect to said key store, configured to determine whether the private key of at least one of the cryptographic key pairs is permitted to be provided to a requester (see Column 2, lines 41-52 and also Column 5 lines 2-10).

wherein the access manager is configured to require that the requester the private key to access a secured electronic file (see Column 2, lines 51-52), and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs (See Column 2, lines 55-56).

Baltzley directly encrypt the electronic file using the public key and therefore does not teach that a data portion of the secured electronic file was previously secured

using a document key and wherein the document key was previously secured by the public key of the cryptographic key pair.

However, hybrid encryption was well-known at the time invention was made. Angelo discloses encrypting the message using a document key and the encrypting the document key using a public key (see, Column 3, lines 13-22).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, instead of public key directly encrypting the documents in the system of Baltzley, the technique of hybrid encryption as taught by Angelo because encrypting the message with the symmetric algorithm is faster then asymmetric algorithm and using public key just to encrypt the document key reduces the chances for plaintext attacks. In other words, hybrid encryption provides the security of public-key encryption at the same time processing messages faster then asymmetric encryption by using symmetric key for data encryption.

Baltzley does not disclose a cryptographic key that pertains to a predetermined time, being uniquely generated each day.

Friedman discloses cryptographic key that pertains to a predetermined time, being uniquely generated each day (see, Paragraph 0149).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to generate and update, cryptographic key in the system of Baltzley, as taught by Friedman because changing the encryption key everyday enhances the security the system compare to the system with static encryption key.

The combination of Baltzley, Angelo, and Friedman discloses encrypting the document with a document key and encrypting the document key with the public key of at least one of the cryptographic key pairs pertaining to the predetermined time. However, the combination does not explicitly discloses encrypted header including the encrypted document key and encrypted access rules for the secured electronic file, the access rules for further protecting the document key and provide restrictive access to the data.

However, Narasimhalu discloses an encrypted header with encrypted document key (see, Fig. 2, Numeral 41 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device.") and encrypted access rules (see, Fig. 2, Numerals 37, 38, 39 and 36 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device."), the

access rules for further protecting the document key and provide restrictive access to the data portion (see, Column 7, lines 29-65, "Next in step 90, the Controller 45 checks whether there are any legal access left by testing the value of LAL 38 for zero. If there are no legal accesses left, the value of LAL 38=0 and an evade processing module is invoked in step 92 which either denies the information access or erases the contents of the medium. The specific action depends on a particular embodiment of the invention. Should the value of LAL be greater than zero, then the Controller 45 compares in step 94 the value of the access window AW 37 with the time of the clock 55. If the current time falls outside of the boundary of the AW 37, the evade processing module in step 92 is invoked. Otherwise, the Controller 45 checks in step 96 whether the medium signature 36 corresponds with the signature read from the input channel 27 and that of the output channel 29. If the medium signature 36 does not match, the sealed COIN is stored on a copied medium. An evade processing module as in step 92 is invoked. Otherwise, the Controller 45 confirms that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium…After the Controller 45 determines that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium in FIG. 5A, the controller extracts in step 95 the encryption /decryption key $K_{TAL\text{-}LAL+1}$ from the header 35.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place the document key of the combined system of Baltzley, Angelo, and Friedman into a header and further append access rules as taught by Narasimhalu with document key into the header because "Digital information is

structured logically to incorporate usage history and allowable access window before it is encrypted in a header portion and a body portion. The end user accesses the digital information with a tamper-proof controlled information access device by decrypting the digital information. A controller disposed in the controlled information access device permits end users to access transparently uncontrolled information." (see, Column 2, line 59-67).

Regarding **Claim 3**, the rejection of claim 1 is incorporated and Baltzley further discloses wherein the requester is a client module that is configured to operatively connect to said access manager over a network (see Figs. 3 and 4).

Claims 2 and 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley in view of Angelo, Friedman Narasimhalu and further in view of Batten-Carew et al. (US 6,603,857 B1), hereinafter "Batten-Carew"

Regarding **Claim 2**, the rejection of claim 1 is incorporated and Baltzley does not teach an access manager is configured to provide the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requester in response to determining that the predetermined time is earlier than or equal to the current time.

Batten-Carew discloses a system, wherein said access manager only provides the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requester in response to determining that the predetermined time is earlier than or equal to the Current time (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 4**, the rejection of claim 1 is incorporated and Baltzley does not discloses a system wherein said document security system further comprises: at least one client module, said client module assists a user in selecting the predetermined time, and said client module secures the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file.

Batten-Carew discloses a system wherein a document security system further comprises: at least one client module, said client module configured to select the predetermined time and secure the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at

any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Baltzley does not disclose wherein said client module further assists in unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time from said key store, and then unsecure the secured electronic file using the private key that pertaining to the predetermined time

Batten-Carew discloses a system wherein said client module further assists in unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time from said key store, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time (Fig. 3 and Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Claims 6-7, 10-12, 16-17, 20, 26, 27, 29, 30 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over En-Seung et al. (US 6,892,306 B1), hereinafter, "En-Seung" in view of Narasimhalu and Friedman.

Regarding **Claims 6, 26 and 29**, En-Seung discloses an apparatus, a corresponding method and a corresponding computer program for controlling release of time-sensitive information, said method comprising:

Identifying an electronic document to be secured, the electronic document having at least a data portion that contains data (see, Column 5, lines 57-61);

generating a access key (see Column 9, lines 9-11);

securing the data portion of the electronic document through use a document key to produce a secured electronic document (see Column 3, lines 14-22 and see Figs. 10 and also Column 5, lines 19-27);

storing the document key in the header portion of the electronic document (see, Column 5, lines 6-8);

securing the header portion of the electronic document through the use of the user key (see, Column 5, lines 6-8)

storing the secured electronic document (see Column 6, lines 54-59).

En-Seung discloses a header portion containing the document key but does not explicitly discloses that the header portion is encrypted and contains both encrypted document key and encrypted access rules wherein the access rules are provided for further protecting the document key and provide restrictive access to the data.

However, Narasimhalu discloses an encrypted header with encrypted document key (see, Fig. 2, Numeral 41 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device.") and encrypted access rules (see, Fig. 2, Numerals 37, 38, 39 and 36 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device."), the access rules for further protecting the document key and provide restrictive access to the data portion (see, Column 7, lines 29-65, "Next in step 90, the Controller 45 checks whether there are any legal access left by testing the value of LAL 38 for zero. If there are no legal accesses left, the value of LAL 38=0 and an evade processing module is invoked in step 92 which either denies the information access or erases the contents of the medium. The specific action depends on a particular embodiment of the invention. Should the value of LAL be greater than zero, then the Controller 45 compares in step

94 the value of the access window AW 37 with the time of the clock 55. If the current time falls outside of the boundary of the AW 37, the evade processing module in step 92 is invoked. Otherwise, the Controller 45 checks in step 96 whether the medium signature 36 corresponds with the signature read from the input channel 27 and that of the output channel 29. If the medium signature 36 does not match, the sealed COIN is stored on a copied medium. An evade processing module as in step 92 is invoked. Otherwise, the Controller 45 confirms that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium...After the Controller 45 determines that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium in FIG. 5A, the controller extracts in step 95 the encryption /decryption key $K_{TAL\text{-}LAL+1}$ from the header 35.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place the document key of the system of En-Seung into a header and further append access rules as taught by Narasimhalu with document key into the header because "Digital information is structured logically to incorporate usage history and allowable access window before it is encrypted in a header portion and a body portion. The end user accesses the digital information with a tamper-proof controlled information access device by decrypting the digital information. A controller disposed in the controlled information access device permits end users to access transparently uncontrolled information." (see, Column 2, line 59-67).

The combination of En-Seung and Narasimhalu discloses user key that encrypt document key and document key in the header that encrypts the contents. However,

En-Seung does not explicitly disclose that the user key is a time-based access key, being uniquely generated each day.

Friedman discloses time-based cryptographic key, being uniquely generated each day (see, Paragraph 0149).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to generate and update, cryptographic key in the system of En-Seung and Narasimhalu, as taught by Friedman because changing the encryption key everyday enhances the security the system compare to the system with static encryption key.

Regarding **Claims 7 and 27**, the combination of En-Seung, Narasimhalu and Friedman further discloses a method wherein the time-based access key has an access time associated therewith (see, Paragraph 0149).

Regarding **Claims 10 and 30**, En-Seung discloses a method and a corresponding computer program for restricting access to an electronic document, said method comprising:

Identifying an electronic document (digital information) to be secured, the electronic document to be secured, the electronic document having at least a data portion that contains data (Column 5, lines 57-61);

obtaining a document key (See Column 3, lines 25-28, "temporary validation key");

encrypting the data portion of the electronic document using the document key to produce an encrypted data potion (see Column 3, lines 25-28);

obtaining an access key (See Column 3, lines 14-22, user key);

storing the access key in the header portion (see, Column 5, lines 6-8);

encrypting the document key using an access key to produce an encrypted document key (see Column 3, lines 14-22, temporary validation key in the header is encrypted using user key);

storing the encrypted document key in the header portion (see, Column 5, lines 6-8);

forming a secured electronic document from at least the encrypted data portion and the header (see Figs. 10 and also Column 5, lines 6-8).

storing the secured electronic document (see Column 6, lines 54-59)

En-Seung discloses a header portion containing the document key but does not explicitly discloses that the header portion includes encrypted document key along with encrypted access rules for the electronic document and wherein the access rules are provided for further protecting the document key.

and provide restrictive access to the data.

However, Narasimhalu discloses an encrypted header with encrypted document key (see, Fig. 2, Numeral 41 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6,

lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device.") and encrypted access rules (see, Fig. 2, Numerals 37, 38, 39 and 36 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device."), the access rules for further protecting the document key and provide restrictive access to the data portion (see, Column 7, lines 29-65, "Next in step 90, the Controller 45 checks whether there are any legal access left by testing the value of LAL 38 for zero. If there are no legal accesses left, the value of LAL 38=0 and an evade processing module is invoked in step 92 which either denies the information access or erases the contents of the medium. The specific action depends on a particular embodiment of the invention. Should the value of LAL be greater than zero, then the Controller 45 compares in step 94 the value of the access window AW 37 with the time of the clock 55. If the current time falls outside of the boundary of the AW 37, the evade processing module in step 92 is invoked. Otherwise, the Controller 45 checks in step 96 whether the medium signature 36 corresponds with the signature read from the input channel 27 and that of the output channel 29. If the medium signature 36 does not match, the sealed COIN is

stored on a copied medium. An evade processing module as in step 92 is invoked. Otherwise, the Controller 45 confirms that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium...After the Controller 45 determines that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium in FIG. 5A, the controller extracts in step 95 the encryption /decryption key $K_{TAL\text{-}LAL+1}$ from the header 35.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place the document key of the system of En-Seung into a header and further append access rules as taught by Narasimhalu with document key into the header because "Digital information is structured logically to incorporate usage history and allowable access window before it is encrypted in a header portion and a body portion. The end user accesses the digital information with a tamper-proof controlled information access device by decrypting the digital information. A controller disposed in the controlled information access device permits end users to access transparently uncontrolled information." (see, Column 2, line 59-67).

The combination of En-Seung and Narasimhalu discloses user key that encrypt document key and document key that encrypts the contents. However, En-Seung does not explicitly disclose that the user key is a time-based access key, being generated each day.

Friedman discloses time-based cryptographic key, being uniquely generated each day (see, Paragraph 0149).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to generate and update, cryptographic key in the system of En-Seung and Narasimhalu, as taught by Friedman because changing the encryption key everyday enhances the security the system compare to the system with static encryption key.

Regarding **Claim 11**, the combination of En-Seung, Narasimhalu and Friedman further discloses wherein encrypting the document key comprises encrypting the document key using a public time-based access key (see Narasimhalu, Column 6, lines 37-44 as combined with Friedman and En-Seung).

Regarding **Claim 12**, the combination of En-Seung, Narasimhalu and Friedman further discloses wherein encrypting the document key comprises encrypting the document key using a time-based access key that has an access time associated therewith (see Friedman, paragraph 0149 as combined with Narasimhalu, Column 6, lines 37-44)

Regarding **Claims 16 and 31**, En-Seung discloses a method and a corresponding computer program for providing a secured electronic document to a requester, the secured electronic document having at least a header portion, having an encrypted document key and access rules, and an encrypted data portion (see, Fig. 10), said method comprising:

obtaining an access key (See Fig. 21A, Numeral S430, and also Column 3, lines 14-22, user key);

decrypting the document key using the time-based access key (see, Column 15, lines 63-67);

En-Seung discloses a header portion containing the document key but does not explicitly discloses that the header portion also includes encrypted access rules that needs to be decrypted wherein the access to the document key being subject to protection by the access rules.

and provide restrictive access to the data.

However, Narasimhalu discloses an encrypted header with encrypted document key (see, Fig. 2, Numeral 41 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device.") and encrypted access rules (see, Fig. 2, Numerals 37, 38, 39 and 36 and also Column 5, lines 43-52, "The header 35 further comprises a plurality of fields: a medium signature 36, an access window 37 (AW), total number of legal accesses allowed 38 (TAL), the number of legal accesses left 39 (LAL), and TAL number of encryption /decryption keys 41 (K_1 to K_{TAL})." and also Column 6, lines 37-44, "By concatenating AW 37, TAL 38, LAL 39, K_1 to K_{TAL} 41, and medium signature 36 as illustrated in FIG. 2, the header 35 is then encrypted in step 68 using the public key DPK of the information consumer's access device."), the

access rules for further protecting the document key and provide restrictive access to the data portion (see, Column 7, lines 29-65, "Next in step 90, the Controller 45 checks whether there are any legal access left by testing the value of LAL 38 for zero. If there are no legal accesses left, the value of LAL 38=0 and an evade processing module is invoked in step 92 which either denies the information access or erases the contents of the medium. The specific action depends on a particular embodiment of the invention. Should the value of LAL be greater than zero, then the Controller 45 compares in step 94 the value of the access window AW 37 with the time of the clock 55. If the current time falls outside of the boundary of the AW 37, the evade processing module in step 92 is invoked. Otherwise, the Controller 45 checks in step 96 whether the medium signature 36 corresponds with the signature read from the input channel 27 and that of the output channel 29. If the medium signature 36 does not match, the sealed COIN is stored on a copied medium. An evade processing module as in step 92 is invoked. Otherwise, the Controller 45 confirms that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium…After the Controller 45 determines that the Information Consumer 30 has a right to access the sealed COIN on the distribution medium in FIG. 5A, the controller extracts in step 95 the encryption /decryption key $K_{TAL\text{-}LAL+1}$ from the header 35.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place the document key of the system of En-Seung into a header and further append access rules as taught by Narasimhalu with document key into the header because "Digital information is structured logically to incorporate

usage history and allowable access window before it is encrypted in a header portion and a body portion. The end user accesses the digital information with a tamper-proof controlled information access device by decrypting the digital information. A controller disposed in the controlled information access device permits end users to access transparently uncontrolled information." (see, Column 2, line 59-67).

The combination of En-Seung and Narasimhalu further discloses:

decrypting an encrypted data portion of the secured electronic document using the document key to produce a non-encrypted data portion (see, Column 16, lines 10-14); and

supplying the non-encrypted data portion to the requester (see, Fig. 21B, Numeral S470).

The combination of En-Seung and Narasimhalu discloses user key that encrypt document key and document key that encrypts the contents. However, En-Seung does not explicitly disclose that the user key is a time-based access key.

Friedman discloses time-based cryptographic key, being uniquely generated each day (see, Paragraph 0149).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to generate and update, cryptographic key in the system of En-Seung and Narasimhalu, as taught by Friedman because changing the encryption key everyday enhances the security the system compare to the system with static encryption key.

Regarding **Claim 17**, the combination of En-Seung, Narasimhalu and Friedman further discloses wherein obtaining a time-based access key comprises obtaining a time-based access key is identified by an indicator within a header portion of the secured electronic document (see, En-Seung Column 15, lines 35-51 as modified by Friedman).

Regarding **Claim 20**, the combination of En-Seung, Narasimhalu and Friedman further discloses wherein said obtaining of the time-based access key is dependent on a current time (see Friedman, Paragraph 0149).

Claims 8, 9, 13-15, 18, 19, 21, 22 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over En-Seung in view of Narasimhalu and Friedman and further in view of Batten-Carew.

Regarding **Claims 8, 13 and 28**, the combination of En-Seung, Narasimhalu and Friedman does not explicitly disclose storing the time-based access key at a remote key store, and wherein the time-based access key is subsequently retrievable from the remote key store only if the current time equal to or later than the access time associated with the time-based access key.

Batten-Carew discloses storing the time-based access key at a remote key store, and wherein the time-based access key is subsequently retrievable from the remote key store only if the current time equal to or later than the access time associated with the time-based access key (see, Fig. 1 and Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of En-Seung, Narasimhalu and Friedman. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 14**, the combination of En-Seung, Narasimhalu, Friedman and Batten-Carew further discloses obtaining a time-based access key comprises obtaining a time-based access key that specifies an access time as a specified day of a year and further comprising obtaining a different unique time-based access keys for a plurality of different days of the year (see, Batten-Carew, Fig. 2 and Column 3, lines 34-40).

Regarding **Claims 9 and 15**, the combination of En-Seung, Narasimhalu, Friedman and Batten-Carew discloses a method wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network (see, Batten-Carew, Fig. 1, Column 3, lines 32-52).

Regarding **Claim 21**, the combination of En-Seung, Narasimhalu and Friedman does not explicitly disclose wherein the time-based access key is associated with an access time, and wherein said obtaining of the time-based access key is permitted when the current time is greater than or equal to the access time see, Fig. 1 and Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of En-

Seung, Narasimhalu and Friedman. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 22**, the combination of En-Seung, Narasimhalu, Friedman, and Batten-Carew further discloses wherein, obtaining a time-based access key comprises obtaining the time based access key from a server (see Batten-Carew, Fig. 1, Column 3, lines 32-52).

Regarding **Claim 18**, the combination of En-Seung, Narasimhalu and Friedman does not explicitly disclose further discloses wherein obtaining a time based access key comprises obtaining a private time-based access key.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). Batten-Carew discloses obtaining a private time-based access key (Column 3, lines 3, lines 48-64).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the private time-based key of Batten-Carew in the combined system of En-Seung, Narasimhalu and Friedman. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific

future time (column 2 lines 29-33). Furthermore, using a private time-based key would extend the benefits of the time based access to the public key encryption scheme.

Regarding **Claim 19**, the combination of En-Seung, Narasimhalu and Friedman further discloses wherein obtaining a time-based access key comprises acquiring the time-based access key from a server (see, Batten-Carew, Fig. 1, Column 3, lines 32-52).

Claims 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over En-Seung in view of Narasimhalu and Friedman and further in view of Bryan et al. (US 2003/0084280 A1), hereinafter, "Bryan".

Regarding Claims 32, 33 and 34, the rejections of claims 6, 26 and 29 is incorporated and even though the combination of En-Seung, Narasimhalu and Friedman discloses generating time-based access key for a predetermined time it does not explicitly discloses a step of determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time. The combination is missing the step of checking to see if the time-based access key is already generated and only generate new time-based access key if one is not available.

Bryan discloses a condition where prior to generating a key, system checks to see the key is already generated and only generates a new key if one is not available (see Paragraph 0026).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to generate, the time-based access key of the combined

system of En-Seung, Narasimhalu and Friedman, only if the key is not available as taught by Bryan. One of ordinary skill in the art would have been motivated to check this condition prior to generating new time-based access key in a case where sender is sending more than one document and all document are supposed to release on the same time. In such a condition it would be appropriate to simply use the same time-based access key rather than generating multiple time-based access keys for the same predetermined time.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F 9:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 5712723859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/YOGESH PALIWAL/
Examiner, Art Unit 2435